IDEAL INDUSTRIES, INC.
AUDACY® SECURITY FRAMEWORK USERS GUIDE

JUNE 2018

PURPOSE: The purpose of this document is to lay out the framework for deploying the Audacy platform into secure environments where data integrity and sensitivity is a concern. In this document we will be discussing a number of topics related to what inherent security options the Audacy platform provides, as well as reviewing what infrastructure precautions should be taken to secure the Audacy environment.

THE AUDACY PLATFORM ARCHITECTURE

The Audacy platform is built and designed to be a simple, easily deployable solution to provide wireless automation and control of your lighting systems. The Audacy platform - hardware (controllers) and software - is a proprietary system that allows for user control and management of sensors, switches, controllers and devices within a given environment. While many solutions in the marketplace today use open protocols like Zigbee, Bluetooth, Z-Wave, and others, the Audacy platform is built on a proprietary protocol to support high performance, scalable Radio Frequency (RF) control and management of wireless controllers. By using a proprietary protocol, the Audacy platform maintains its own closed format for data distribution between the software management layer all the way down to the physical hardware controllers deployed for lighting and Building Automation System (BAS) integration. This includes but is not limited to proprietary modulation schemes for wireless transmission, pseudo-random encoding for QPSK, and private key encryption support. In addition, all communication has the ability to be encrypted (differs between communications channels) such that information exchange and control is only available to those systems that have proper authorization into the system itself.

Client access to the system is only granted with the proper username and password, and full TLS based encryption is provided for all client to server communications. Internal components designed specifically for the Audacy system also provide a binary level of encryption between components within the infrastructure that allows for a simple layer of security between these front end systems all the way down to the backend Audacy Gateways and controllers themselves.

SECURING THE AUDACY ENVIRONMENT

While the Audacy platform is constantly implementing and improving information security within the system itself, there are a number of deployment recommendations IDEAL INDUSTRIES, INC. strongly encourages clients implement when deploying the Audacy platform. Client deployments have differing expertise and knowledge around information security so this section is designed to provide a basic overview of securing the infrastructure used to deploy the Audacy components.

The Audacy system has a number of unique components that are used to manage and control fixtures, sensors and switches. The primary component that is used for managing these controllers is the Audacy Gateway. The Gateway provides RF control and management of the physical controller hardware as well as provides integration with the user front end controls (web and iOS applications) and third party solutions (BAS). The Audacy Gateway is designed to be deployed in the client environment and requires a network (RJ45 Ethernet) connection into the physical networking infrastructure of the client deployment. Most clients already have a separate isolated (either virtual or physical) network segment for managing facilities infrastructure (HVAC, BAS, Lighting, Building Security, etc.). IDEAL highly recommends deploying the Audacy system into a separate isolated (either virtual or physical) network segment from core IT services (financial data, personal data, production IT infrastructure, etc.). This segmentation, while having performance and operational benefits, also provides an additional layer of security by isolating the Audacy system from other highly sensitive data.

In addition, when the Audacy platform is deployed to integrate with backend Building Automation Systems (BAS), Audacy uses standards-based integration over BACnet and is fully BACnet certified. Clients wishing to secure integration with backend BAS systems should review their BACnet security model and policies to ensure they have properly integrated the Audacy platform over BACnet communications.

The Audacy platform also allows for behind-the-firewall operation where the Gateway is deployed into the client's infrastructure but is not open to communication outside the firewall. A proxy server is used for securing communications between the Gateway and the cloud-based Audacy Controls Interface. The proxy server should be deployed into the client's network DMZ allowing for aggregation of outbound secure traffic to the Audacy Controls Interface and securing inbound communication to the Gateway.

In all cases of data security, one of the most overlooked areas is actual physical security of the system itself. At a minimum, IDEAL INDUSTRIES, INC. highly recommends that in secure environments, physical security and surveillance be implemented around deployment of the Gateway and the Audacy Proxy services. These components should always be deployed into physically secure environments that provide proper access control and surveillance of the infrastructure deployed.

DEPLOYMENT OF THE AUDACY SYSTEM

It should be noted that in all cases, the Audacy system should never be deployed into environments where it has direct oversight of systems that could result in death or personal injury.

Please see IDEAL INDUSTRIES, INC. Limitation of Liability clause in our warranty statement for further details.

1.800.273.9989

CONTACTUS@AUDACYWIRELESS.COM

AUDACYWIRELESS.COM

AUDACY®
WIRELESS LIGHTING CONTROL
YOUR WORLD IN A BETTER LIGHT
A DIVISION OF IDEAL INDUSTRIES, INC.